**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Информационная безопасность и защита информации в сетях ЭВМ

Уровень образования: **высшее образование - магистратура**
Направление подготовки (специальность): **27.04.04 Управление в технических системах**
Направленность (профиль): **Управление и автоматизация технологических процессов и производств**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**
Курс: **2**
Семестр: **3**
Учебный план набора 2015 года

Распределение рабочего времени

| № | Виды учебной деятельности | 3 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 12 | 12 | часов |
| 2 | Практические занятия | 16 | 16 | часов |
| 3 | Лабораторные работы | 16 | 16 | часов |
| 4 | Всего аудиторных занятий | 44 | 44 | часов |
| 5 | Из них в интерактивной форме | 20 | 20 | часов |
| 6 | Самостоятельная работа | 64 | 64 | часов |
| 7 | Всего (без экзамена) | 108 | 108 | часов |
| 8 | Общая трудоемкость | 108 | 108 | часов |
| | | 3.0 | 3.0 | З.Е |

Зачет: 3 семестр

Томск 2017

Согласована на портале № 21577

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 8 » 6 2017 г.

# ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 27.04.04 Управление в технических системах, утвержденного 30 октября 2014 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

ассистент каф. КИБЭВС _____ А. К. Новохрестов

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФВС _____ Л. А. Козлова

Заведующий выпускающей каф.
КСУП _____ Ю. А. Шурыгин

Эксперт:

доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 21577

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

### 1.2. Задачи дисциплины

- Дать основы:
- – архитектуры вычислительных сетей;
- – программно-аппаратных и технических средств создания сетей;
- – принципов построения сетей и управления ими;
- – использования программных и аппаратных технологий защиты сетей;
- – методологии проектирования, развертывания и сопровождения безопасных сетей;
- – обследования и анализа защищенных вычислительных сетей.
-

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность и защита информации в сетях ЭВМ» (Б1.В.ОД.6) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Компьютерные технологии управления в технических системах, Менеджмент в телекоммуникационных системах.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-4 способностью адаптироваться к изменяющимся условиям, переоценивать накопленный опыт, анализировать свои возможности;
- ПК-5 способностью анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем, готовить научные публикации и заявки на изобретения;
- ПСК-3 способностью обеспечить защиту информации в системах АСУ ТП;

В результате изучения дисциплины студент должен:

- **знать** средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.
- **уметь** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.
- **владеть** навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 3 семестр |

Согласована на портале № 21577

| | | |
|---|---|---|
| Аудиторные занятия (всего) | 44 | 44 |
| Лекции | 12 | 12 |
| Практические занятия | 16 | 16 |
| Лабораторные работы | 16 | 16 |
| Из них в интерактивной форме | 20 | 20 |
| Самостоятельная работа (всего) | 64 | 64 |
| Оформление отчетов по лабораторным работам | 42 | 42 |
| Проработка лекционного материала | 12 | 12 |
| Подготовка к практическим занятиям, семинарам | 10 | 10 |
| Всего (без экзамена) | 108 | 108 |
| Общая трудоемкость ч | 108 | 108 |
| Зачетные Единицы | 3.0 | 3.0 |

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|---|
| 3 семестр | | | | | | |
| 1 Основные понятия информационной безопасности | 2 | 0 | 0 | 2 | 4 | ОК-4, ПК-5 |
| 2 Технологии обеспечения безопасности в локальных сетях | 3 | 16 | 4 | 25 | 48 | ОК-4, ПК-5, ПСК-3 |
| 3 Обеспечение безопасности сетей на базе сетевых операционных систем | 2 | 0 | 0 | 2 | 4 | ОК-4, ПК-5, ПСК-3 |
| 4 Обеспечение безопасности межсетевого взаимодействия | 3 | 0 | 12 | 33 | 48 | ОК-4, ПК-5, ПСК-3 |
| 5 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот | 2 | 0 | 0 | 2 | 4 | ОК-4, ПК-5, ПСК-3 |
| Итого за семестр | 12 | 16 | 16 | 64 | 108 | |
| Итого | 12 | 16 | 16 | 64 | 108 | |

Согласована на портале № 21577

**5.2. Содержание разделов дисциплины (по лекциям)**

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 3 семестр | | | |
| 1 Основные понятия информационной безопасности | Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология. | 1 | ОК-4, ПК-5 |
| | Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность. | 1 | |
| | Итого | 2 | |
| 2 Технологии обеспечения безопасности в локальных сетях | Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование. | 1 | ПСК-3, ПК-5 |
| | Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. | 1 | |
| | Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях. | 1 | |
| | Итого | 3 | |
| 3 Обеспечение безопасности сетей на базе сетевых операционных систем | Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля. | 1 | ПСК-3 |
| | Политика безопасности: Понятие политики безопасности. Типовые элементы политики безопасности. Построение, реализация, поддержание и модификация политики безопасности.Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа. | 1 | |

Согласована на портале № 21577

| | | | |
|---|---|---|---|
| | Итого | 2 | |
| 4 Обеспечение безопасности межсетевого взаимодействия | Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет. | 1 | ПК-5 |
| | Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети. | 1 | |
| | Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. | 1 | |
| | Итого | 3 | |
| 5 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот | Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности. | 1 | ПК-5, ПСК-3 |
| | Классы сканеров безопасности и особенности применения. Защита от вирусов.Защита электронного документооборота. | 1 | |
| | Итого | 2 | |
| Итого за семестр | | 12 | |

**5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами**

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Предшествующие дисциплины | | | | | |
| 1 Компьютерные технологии управления в технических системах | + | | | | |
| 2 Менеджмент в телекоммуникационных системах | | + | | + | |

**5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий**

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| | Виды занятий | Формы контроля |
|---|---|---|

Согласована на портале № 21577

| Компетенции | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | |
|---|---|---|---|---|---|
| ОК-4 | + | + | | + | Защита отчета, Опрос на занятиях |
| ПК-5 | + | + | | + | Защита отчета, Опрос на занятиях |
| ПСК-3 | + | + | + | + | Защита отчета, Отчет по лабораторной работе, Опрос на занятиях |

## 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

| Методы | Интерактивные практические занятия | Интерактивные лабораторные занятия | Интерактивные лекции | Всего |
|---|---|---|---|---|
| 3 семестр | | | | |
| IT-методы | | 8 | | 8 |
| Презентации с использованием слайдов с обсуждением | | | 6 | 6 |
| Исследовательский метод | 6 | | | 6 |
| Итого за семестр: | 6 | 8 | 6 | 20 |
| Итого | 6 | 8 | 6 | 20 |

## 7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 3 семестр | | | |
| 2 Технологии обеспечения безопасности в локальных сетях | Разграничение доступа к локальным и сетевым ресурсам. Дискреционная и мандатная модели управления доступом. | 2 | ПСК-3 |
| | Инструменты для исследования сети (сниферы) | 1 | |

Согласована на портале № 21577

| | | | |
|---|---|---|---|
| | Инструменты для исследования сети (сканеры безопасности) | 1 | |
| | Итого | 4 | |
| 4 Обеспечение безопасности межсетевого взаимодействия | Межсетевые экраны | 2 | ПСК-3 |
| | Антивирусная защита | 2 | |
| | Виртуальные частные сети | 2 | |
| | Системы обнаружения и предотвращения вторжений | 2 | |
| | DLP-системы | 2 | |
| | Безопасность прикладных протоколов | 2 | |
| | Итого | 12 | |
| Итого за семестр | | 16 | |

## 8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 3 семестр | | | |
| 2 Технологии обеспечения безопасности в локальных сетях | Построение структуры информационной сети, описание характера связей между элементами и информационных потоков. | 4 | ОК-4, ПК-5, ПСК-3 |
| | Проработка модели угроз и модели нарушителя компьютерной сети. | 4 | |
| | Проработка структуры системы защиты информации, состава средств защиты. Изучение способов установки и основных параметров конфигурации средств защиты информации | 4 | |
| | Подготовка документов по системе защиты информации в информационной системе. | 4 | |
| | Итого | 16 | |
| Итого за семестр | | 16 | |

## 9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Согласована на портале № 21577

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 3 семестр | | | | |
| 1 Основные понятия информационной безопасности | Проработка лекционного материала | 2 | ОК-4, ПК-5 | Опрос на занятиях |
| | Итого | 2 | | |
| 2 Технологии обеспечения безопасности в локальных сетях | Подготовка к практическим занятиям, семинарам | 10 | ОК-4, ПК-5, ПСК-3 | Защита отчета, Опрос на занятиях, Отчет по лабораторной работе |
| | Проработка лекционного материала | 3 | | |
| | Оформление отчетов по лабораторным работам | 12 | | |
| | Итого | 25 | | |
| 3 Обеспечение безопасности сетей на базе сетевых операционных систем | Проработка лекционного материала | 2 | ОК-4, ПК-5 | Опрос на занятиях |
| | Итого | 2 | | |
| 4 Обеспечение безопасности межсетевого взаимодействия | Проработка лекционного материала | 3 | ОК-4, ПК-5, ПСК-3 | Опрос на занятиях, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 30 | | |
| | Итого | 33 | | |
| 5 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот | Проработка лекционного материала | 2 | ОК-4, ПК-5 | Опрос на занятиях |
| | Итого | 2 | | |
| Итого за семестр | | 64 | | |
| Итого | | 64 | | |

## 10. Курсовая работа (проект)

Не предусмотрено РУП

## 11. Рейтинговая система для оценки успеваемости студентов

### 11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|---|---|---|---|---|
| 3 семестр | | | | |
| Защита отчета | 15 | 15 | | 30 |

Согласована на портале № 21577

| | | | | |
|---|---|---|---|---|
| Опрос на занятиях | 10 | 10 | 10 | 30 |
| Отчет по лабораторной работе | | 20 | 20 | 40 |
| Итого максимум за период | 25 | 45 | 30 | 100 |
| Нарастающим итогом | 25 | 70 | 100 | 100 |

### 11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

| Баллы на дату контрольной точки | Оценка |
|---|---|
| ≥ 90% от максимальной суммы баллов на дату КТ | 5 |
| От 70% до 89% от максимальной суммы баллов на дату КТ | 4 |
| От 60% до 69% от максимальной суммы баллов на дату КТ | 3 |
| < 60% от максимальной суммы баллов на дату КТ | 2 |

### 11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|
| 5 (отлично) (зачтено) | 90 - 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 - 89 | B (очень хорошо) |
| | 75 - 84 | C (хорошо) |
| | 70 - 74 | D (удовлетворительно) |
| 3 (удовлетворительно) (зачтено) | 65 - 69 | |
| | 60 - 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

## 12. Учебно-методическое и информационное обеспечение дисциплины

### 12.1. Основная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). - Алф. указ.: с. 918-943. - ISBN 978-5-496-00004-8 : 470.69 р. (наличие в библиотеке ТУСУР - 20 экз.)

2. Компьютерные сети [Текст] : научное издание / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : ПИТЕР, 2013. - 960 с. : ил., табл. - (КЛАССИКА COMPUTER SCIENCE). - Пер. с англ. - Алф. указ.: с. 947-955. - ISBN 978-5-4461-0068-2 : 1244.32 р. (наличие в библиотеке ТУСУР - 15 экз.)

### 12.2. Дополнительная литература

1. Сетевые операционные системы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538[6] с. : ил. - (Учебник для вузов). - Библиогр.: с. 525-526. - Алф. указ.: с. 527-538. - ISBN 5-272-00120-6 : 145.20 р. (наличие в библиотеке ТУСУР - 10 экз.)

Согласована на портале № 21577

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf
2. Безопасность сетей ЭВМ: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf

#### 12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

### 12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://www.lib.tusur.ru – библиотека университета;
2. http://www.elibrary.ru – научная электронная библиотека;
3. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
4. 
5. Программное обеспечение:
6. операционные системы семейства Windows;
7. средство защиты информации "Блокхост-сеть К";
8. система обнаружения вторжений "Snort";
9. средство моделирования сетей Cisco Packet Tracer;
10. DLP-система "Контур информационной безопасности SearchInform";
11. дистрибутив Kali Linux;
12. система анализа защищенности сети "MaxPatrol".

## 13. Материально-техническое обеспечение дисциплины

### 13.1. Общие требования к материально-техническому обеспечению дисциплины

#### 13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

#### 13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/ HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.;

Согласована на портале № 21577

Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

**13.1.3. Материально-техническое обеспечение для лабораторных работ**

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/ HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

**13.1.4. Материально-техническое обеспечение для самостоятельной работы**

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

**13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья**

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

## 14. Фонд оценочных средств

**14.1. Основные требования к фонду оценочных средств и методические рекомендации**

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

**14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья**

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

| Категории студентов | Виды дополнительных оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, | Преимущественно письменная проверка |

Согласована на портале № 21577

| | | |
|---|---|---|
| | контрольные работы | |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

### 14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 21577

**Приложение 1**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

# Информационная безопасность и защита информации в сетях ЭВМ

Уровень образования: **высшее образование - магистратура**
Направление подготовки (специальность): **27.04.04 Управление в технических системах**
Направленность (профиль): **Управление и автоматизация технологических процессов и производств**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**
Курс: **2**
Семестр: **3**

Учебный план набора 2015 года

Разработчик:
- ассистент каф. КИБЭВС А. К. Новохрестов

Зачет: 3 семестр

Томск 2017

Согласована на портале № 21577

## 1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенций |
|---|---|---|
| ОК-4 | способностью адаптироваться к изменяющимся условиям, переоценивать накопленный опыт, анализировать свои возможности | Должен знать средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. ;<br>Должен уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов. ;<br>Должен владеть навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений. ; |
| ПК-5 | способностью анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем, готовить научные публикации и заявки на изобретения | |
| ПСК-3 | способностью обеспечить защиту информации в системах АСУ ТП | |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|---|---|---|---|

Согласована на портале № 21577

| | | | |
|---|---|---|---|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования | Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем |
| Удовлетворительно (пороговый уровень) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми для выполнения простых задач | Работает при прямом наблюдении |

## 2 Реализация компетенций

### 2.1 Компетенция ОК-4

ОК-4: способностью адаптироваться к изменяющимся условиям, переоценивать накопленный опыт, анализировать свои возможности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | способы адаптации к изменяющимся условиям, переоценки накопленного опыта, анализа своих возможностей | адаптироваться к изменяющимся условиям, переоценивать накопленный опыт, анализировать свои возможности | навыками адаптации к изменяющимся условиям, переоценки накопленного опыта, анализа своих возможностей |
| Виды занятий | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Опрос на занятиях;<br>• Зачет; | • Опрос на занятиях;<br>• Зачет; | • Зачет; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|

Согласована на портале № 21577

| | | | |
|---|---|---|---|
| Отлично (высокий уровень) | • способы адаптации к изменяющимся условиям, переоценки накопленного опыта, анализа своих возможностей; | • адаптироваться к изменяющимся условиям, переоценивать накопленный опыт, анализировать свои возможности; | • навыками адаптации к изменяющимся условиям, переоценки накопленного опыта, анализа своих возможностей; |
| Хорошо (базовый уровень) | • способы адаптации к изменяющимся условиям, переоценки накопленного опыта; | • адаптироваться к изменяющимся условиям, переоценивать накопленный опыт; | • навыками адаптации к изменяющимся условиям, переоценки накопленного опыта; |
| Удовлетворительно (пороговый уровень) | • способы адаптации к изменяющимся условиям; | • адаптироваться к изменяющимся условиям; | • навыками адаптации к изменяющимся условиям; |

### 2.2 Компетенция ПК-5

ПК-5: способностью анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем, готовить научные публикации и заявки на изобретения.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | способы анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем, подготовки научных публикаций и заявок на изобретения | анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем, готовить научные публикации и заявки на изобретения | навыками анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем, подготовки научных публикаций и заявок на изобретения |
| Виды занятий | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Опрос на занятиях;<br>• Зачет; | • Опрос на занятиях;<br>• Зачет; | • Зачет; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Согласована на портале № 21577

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • способы анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем, подготовки научных публикаций и заявок на изобретения; | • анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем, готовить научные публикации и заявки на изобретения; | • навыками анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем, подготовки научных публикаций и заявок на изобретения; |
| Хорошо (базовый уровень) | • способы анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем; | • анализировать результаты теоретических и экспериментальных исследований, давать рекомендации по совершенствованию устройств и систем; | • навыками анализа результатов теоретических и экспериментальных исследований, составления рекомендаций по совершенствованию устройств и систем; |
| Удовлетворительно (пороговый уровень) | • способы анализа результатов теоретических и экспериментальных исследований; | • анализировать результаты теоретических и экспериментальных исследований; | • навыками анализа результатов теоретических и экспериментальных исследований; |

### 2.3 Компетенция ПСК-3

ПСК-3: способностью обеспечить защиту информации в системах АСУ ТП.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | способы обеспечения защиты информации в системах АСУ ТП | обеспечить защиту информации в системах АСУ ТП | навыками обеспечения защиты информации в системах АСУ ТП |
| Виды занятий | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Отчет по лабораторной работе;<br>• Опрос на занятиях; | • Отчет по лабораторной работе;<br>• Опрос на занятиях; | • Отчет по лабораторной работе;<br>• Зачет; |

Согласована на портале № 21577

| | | | |
|---|---|---|---|
| | • Зачет; | • Зачет; | |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • на продвинутом уровне способы обеспечения защиты информации в системах АСУ ТП; | • на продвинутом уровне обеспечить защиту информации в системах АСУ ТП; | • на продвинутом уровне навыками обеспечения защиты информации в системах АСУ ТП; |
| Хорошо (базовый уровень) | • способы обеспечения защиты информации в системах АСУ ТП; | • обеспечить защиту информации в системах АСУ ТП; | • навыками обеспечения защиты информации в системах АСУ ТП; |
| Удовлетворительно (пороговый уровень) | • на базовом уровне способы обеспечения защиты информации в системах АСУ ТП; | • на базовом уровне обеспечить защиту информации в системах АСУ ТП; | • на базовом уровне навыками обеспечения защиты информации в системах АСУ ТП; |

## 3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

### 3.1 Темы опросов на занятиях

– Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология.

– Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.

– Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование.

– Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.

– Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

– Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля.

– Политика безопасности: Понятие политики безопасности. Типовые элементы политики безопасности. Построение, реализация, поддержание и модификация политики безопасности.Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа.

– Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет.

– Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети.

– Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.

– Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.

Согласована на портале № 21577

– Классы сканеров безопасности и особенности применения. Защита от вирусов.
– Защита электронного документооборота.

### 3.2 Темы лабораторных работ

– Разграничение доступа к локальным и сетевым ресурсам. Дискреционная и мандатная модели управления доступом.
– Инструменты для исследования сети (сниферы)
– Инструменты для исследования сети (сканеры безопасности)
– Межсетевые экраны
– Антивирусная защита
– Виртуальные частные сети
– Системы обнаружения и предотвращения вторжений
– DLP-системы
– Безопасность прикладных протоколов

### 3.3 Зачёт

– 1. Типовые конфигурации информационных систем. Влияние конфигурации информационной системы на безопасность хранимых, обрабатываемых и передаваемых по сети данных. 2. Угроза. Уязвимость. Атака. Взаимосвязь между этими понятиями. 3. Классификация угроз информационной безопасности вычислительных сетей. 4. Классификация уязвимостей. 5. Классификация атак. 6. Перехват информации в сети. Инструменты. Способы противодействия перехвату. 7. Spoofing. Способы подделки идентификаторов. Способы противодействия spoofing`у. 8. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам. 9. Универсальные методы обеспечения информационной безопасности компьютеров и компьютерных сетей. 10. Специализированные методы обеспечения информационной безопасности компьютерных сетей. 11. Идентификация и аутентификация. Особенности аутентификации пользователей в компьютерных сетях. 12. Протокол Kerberos. Назначение. Особенности функционирования. 13. Разграничение доступа к информационным ресурсам компьютерных сетей. 14. Криптографическая защита информации в компьютерных сетях. Достоинства и недостатки. Способы преодоления криптографической защиты информации. 15. Электронная подпись. Назначение. Применение для защиты сетевого взаимодействия. Примеры. 16. Сканеры безопасности. Способы выявления уязвимостей в информационных системах. 17. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности. 18. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак. 19. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки. 20. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки. 21. Демилитаризованная зоны. Назначение. Способы выделения. 22. Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов. 23. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки. 24. Основные компоненты технологии виртуальных частных сетей (VLAN). 25. Вредоносные программы. Классификация. Каналы распространения. Влияние на информационные системы. 26. Антивирусные средства. Классификация. Методики выявления вредоносного кода. 27. Средства обеспечения информационной безопасности в ОС Windows’2003. Разграничение доступа к данным. Групповая политика. Область действия групповых политик. 28. Основные этапы разработки защищенной компьютерной сети. 29. Проблемы обеспечения безопасности прикладных сервисов (Веб, почта, FTP) и их решения. 30. Физические средства обеспечения информационной безопасности.

## 4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

Согласована на портале № 21577

### 4.1. Основная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). - Алф. указ.: с. 918-943. - ISBN 978-5-496-00004-8 : 470.69 р. (наличие в библиотеке ТУСУР - 20 экз.)
2. Компьютерные сети [Текст] : научное издание / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : ПИТЕР, 2013. - 960 с. : ил., табл. - (КЛАССИКА COMPUTER SCIENCE). - Пер. с англ. - Алф. указ.: с. 947-955. - ISBN 978-5-4461-0068-2 : 1244.32 р. (наличие в библиотеке ТУСУР - 15 экз.)

### 4.2. Дополнительная литература

1. Сетевые операционные системы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538[6] с. : ил. - (Учебник для вузов). - Библиогр.: с. 525-526. - Алф. указ.: с. 527-538. - ISBN 5-272-00120-6 : 145.20 р. (наличие в библиотеке ТУСУР - 10 экз.)

### 4.3. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf
2. Безопасность сетей ЭВМ: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf

### 4.4. Базы данных, информационно справочные и поисковые системы

1. http://www.lib.tusur.ru – библиотека университета;
2. http://www.elibrary.ru – научная электронная библиотека;
3. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
4. 
5. Программное обеспечение:
6. операционные системы семейства Windows;
7. средство защиты информации "Блокхост-сеть К";
8. система обнаружения вторжений "Snort";
9. средство моделирования сетей Cisco Packet Tracer;
10. DLP-система "Контур информационной безопасности SearchInform";
11. дистрибутив Kali Linux;
12. система анализа защищенности сети "MaxPatrol".

Согласована на портале № 21577